StationGuard GridOps

Was ist neu in Version 2.00

Version 2.00

Highlights

1. Statusangabe der Schwachstellenbehandlung

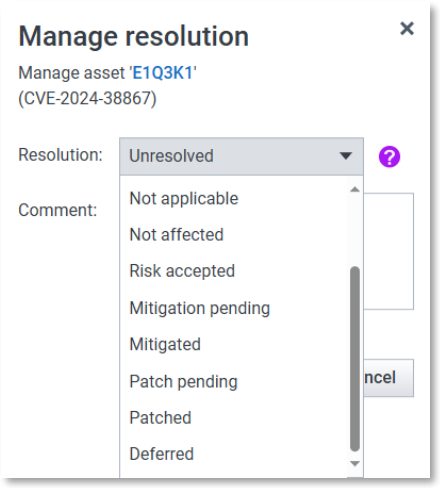
Koordinieren Sie Ihre Reaktion auf exponierte Schwachstellen effizienter mit den folgenden Funktionen:

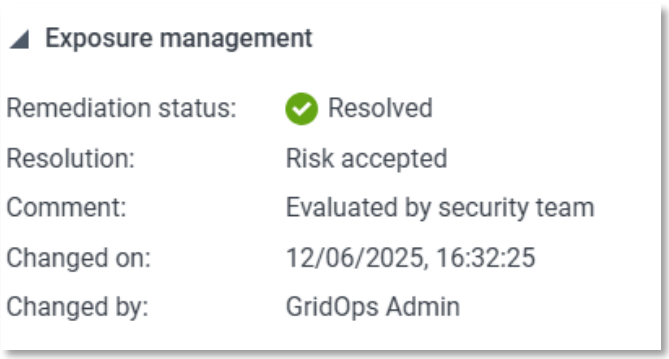
> Verfolgen Sie die Behandlung exponierter Schwachstellen und definieren Sie einfach einen Status für jede einzelne davon, um anzugeben, welche Maßnahmen bereits ergriffen wurden oder zu ergreifen sind:

  > *Unresolved*
  > *Under investigation*
  > *False positive*
  > *Not applicable*
  > *Not affected*
  > *Risk accepted*
  > *Mitigation pending*
  > *Mitigated*
  > *Patch pending*
  > *Patched*
  > *Deferred*

> Sie können jederzeit sehen, wer potenzielle Bedrohungen behandelt hat und wann eine Schwachstellenbehandlung angewendet wurde.

> Es ist möglich, mehrere betroffene Assets gleichzeitig zu verwalten.





2. Schwachstellen-Matching mit verbesserter Präzision

GridOps baut auf unserer branchenführenden Genauigkeit beim Matching von Schwachstellen auf und bietet nun mehrere Verbesserungen, die die Präzision noch weiter steigern:

- **Unterstützung für CSAF-Relationships**: Wir haben die Voraussetzungen geschaffen, um Schwachstellen speziell der betroffenen Hardware einzelner Hersteller zuzuordnen. Somit kann GridOps CSAF-Beziehungen lesen und erkennen, dass bestimmte CVEs von bestimmten Anbietern oft nur einzelne Hardware-Modelle und nicht ganze Produktserien betreffen.

- **Modulspezifisches Schwachstellen-Matching**: GridOps extrahiert den CP-Modultyp aus den Produktcodes der SIEMENS-Geräte, um ein noch genaueres Schwachstellen-Matching zu ermöglichen - insbesondere in Fällen, in denen die CVE-Anwendbarkeit zwischen Basismodulen (z. B. CP100, CP200) und Erweiterungsmodulen variiert.

- Wir haben die Zahl der falsch-positiven Schwachstellen-Matching weiter reduziert, indem wir verfeinerte Filter und Matching-Verfahren eingeführt haben - selbst bei unvollständigen Anlagendaten.

- **GridOps erkennt Variationen von Produktnamen**: Es kann Gerätemodelle selbst dann identifizieren, wenn sie mit unterschiedlichen Namenskonventionen - wie Synonymen, Akronymen und Abkürzungen - aufgeführt sind, und sie genau der richtigen Produktgruppe zuordnen. Dadurch wird die Genauigkeit des Algorithmus zum Matching von Schwachstellen weiter verbessert. Beispiele für Abkürzungen sind:

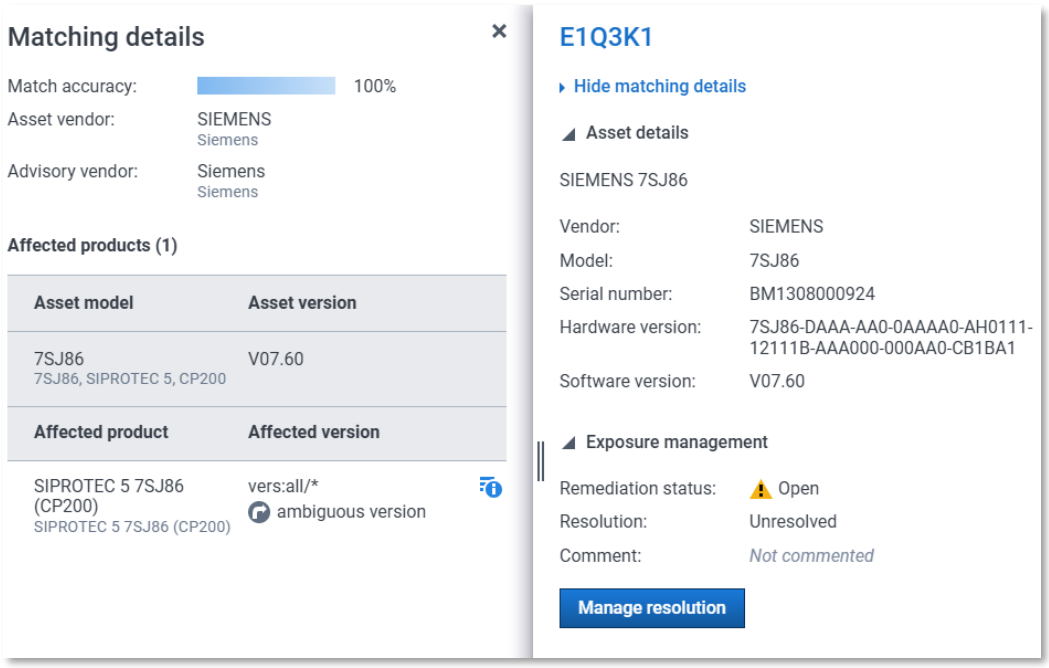
  - **Schneider**
    - Distributed Control System – DCS
    - Tricon Communication Model/Module – TCM
    - Tricon Processor Model/Module – TPM
    - APC PowerChute Network Shutdown – PCNS
  - **Siemens**
    - Totally Integrated Automation – TIA
  - **Hitachi**
    - ASPECT Enterprise - ASP-ENT
    - Harmony OPC Server – HAOPC
  - **Westermo**
    - RedFox Industrial Rack – RFIR
  - **Cisco**
    - Application Policy Infrastructure Controller – APIC
    - Aggregation Services Router – ASR
    - Analog Telephone Adapter – ATA
    - Adaptive Security Appliance – ASA
    - Cisco Secure Firewall – CSF
    - Firepower Management Center – FMC
    - Firepower Threat Defense – FTD
    - Firepower Extensible Operating System – FXOS
    - IoT Field Network Director - IoT FND
    - Integrated Services Router – ISR
    - Network Convergence System – NCS
    - Wide Area Application Services – WAAS
    - WAN Automation Engine – WAE
    - Wireless LAN Controller – WLC

- Falsch-positives Schwachstellen-Matching für A8000-Anlagen wurden erheblich reduziert. Zuvor wurden CP-802x-Modelle auch mit CP-803x abgeglichen, aber die Matching-Logik wurde jetzt verfeinert, um CP-Modelle genauer zu unterscheiden.

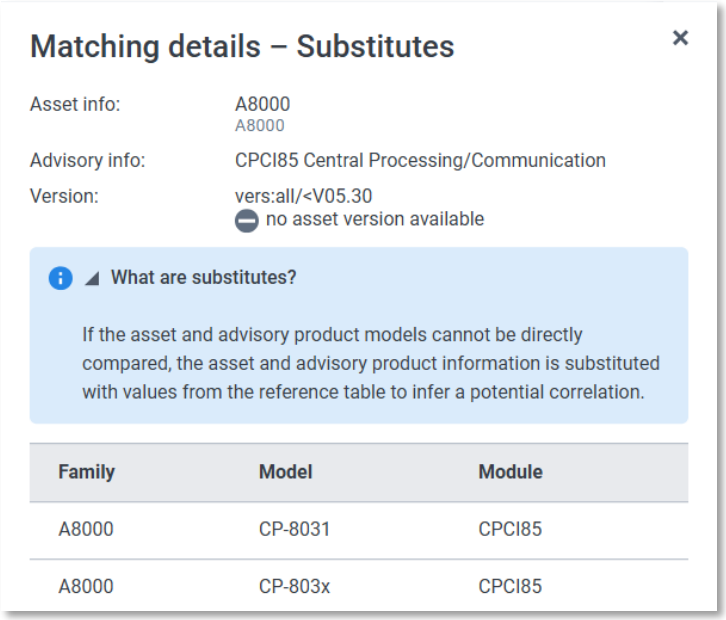
3. Ergänzende Informationen im Schwachstellen-Matching

Zugeordnete Schwachstellen werden mit erweiterten Informationen und einer besseren Transparenz dargestellt:

> **Neue Details beim Schwachstellen-Matching**: Sie erhalten Informationen darüber, warum eine bestimmte Schwachstelle einem Asset zugeordnet wurde. Dies bietet Ihnen tiefere Einblicke in den Matching-Prozess und hilft Ihnen, den Kontext und die Gründe für jedes Schwachstellen-Matching nachzuvollziehen.



> Die *Matching details* wurden um die Option erweitert, *substitutes* anzuzeigen, wenn diese für das Matching eines Produkts verwendet wurden.



4. Kontinuierliche Erweiterung der Schwachstellendatenbank

Unsere Schwachstellen-Datenbank wird ständig erweitert – zuletzt haben wir über 3.000 neue Schwachstellen aus mehr als 1.000 neuen Hinweisen hinzugefügt.

Schwachstellen	Hersteller	Sicherheitshinweise
13.000 +	**39 +**	**5.500 +**

Gesamt: 5. Juli 2025

5. Kontinuierliche Erweiterung der Asset-Typ-Datenbank

Die Asset-Datenbank in GridOps wurde um zusätzliche Gerätehersteller und -familien erweitert. Dies ermöglicht eine genauere Klassifizierung der Geräte nach Typ, Familie und Hersteller, was die Präzision beim Matching von Schwachstellen verbessert.

Dies sind die neu hinzugekommenen Asset-Familien:

- **Schneider**
  - Andover Continuum
  - Sage RTU
  - TCM
  - UCM
  - TPM
  - TriStation
- **Hitachi**
  - SAM-IO
- **Siemens**
  - A8000 modules
  - A8000 / CP-801x
  - DIGSI
  - M969
  - RUGGEDCOM switches (12 series)
  - Reyrolle
  - S7-300 / S7-400 / S7-1500
  - Scalance series (24 series)
  - i800
- **FortiNet**
  - FortiAP
  - FortiGate
  - FortiProxy
  - FortiSwitch
- **Cisco**
  - ASA firmware
  - FTD firmware
  - FXOS firmware
  - NX-OS firmware
  - ASA series
  - ASR series
  - CGS series
  - CSF series
  - Catalyst series
  - Firepower series
  - IE series
  - ISR series
  - MDS series
  - NCS series
  - Nexus series
  - UCS series
- **Phoenix Contact**
  - RS4000
  - PLCnext
- **Rockwell**
  - Kinetix families
  - Stratix families

6. Echtzeit-Sensor-Status

Wir haben die Transparenz des StationGuard Sensors in GridOps verbessert, damit Sie alle Informationen auf einen Blick bekommen.

- Der Status der Sensorverbindung wird nun angezeigt, einschließlich Echtzeit-Updates. Sie finden ihn unter dem Tab *Sensor management*.

- Zusätzlich kann der Status der Sensorverbindung auch im Dashboard *Sensors* eingesehen werden. Dort können Sie auch für jeden einzelnen Sensor sehen, ob der Wartungsmodus aktiviert ist oder nicht.

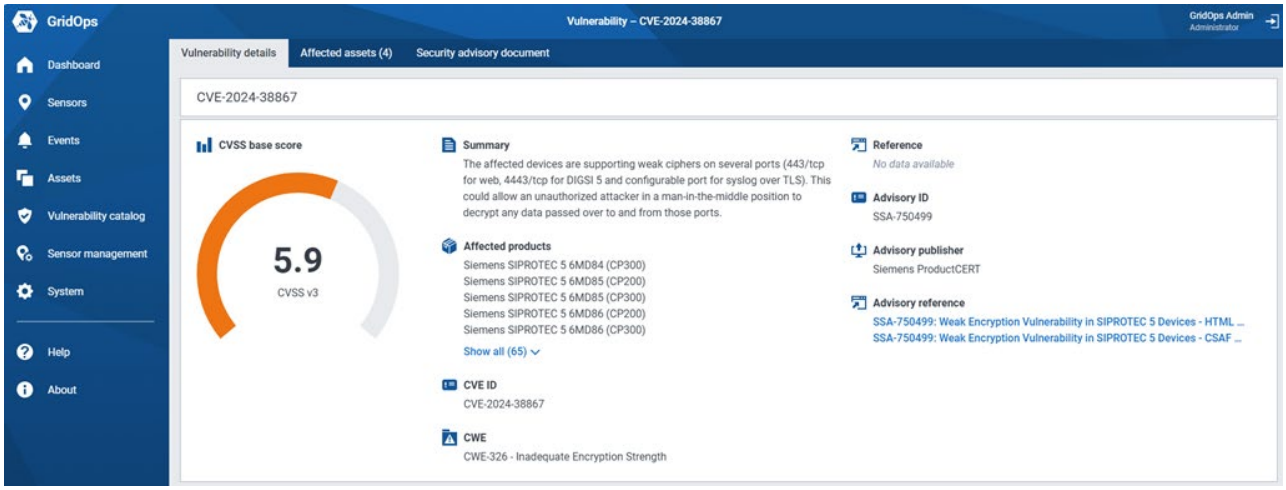
7. Dashboard-Verbesserungen

Wir haben mehrere Verbesserungen an den Dashboards vorgenommen, um klarere Einblicke zu bieten und die Leistungsfähigkeit zu steigern – insbesondere, wenn Sie mit großen Asset-Umgebungen arbeiten:

- Das Dashboard *Event detail* enthält VLAN ID und VLAN Priority für GOOSE-Alarme.
- Neue Panels, die dem Dashboard *Event detail* hinzugefügt wurden:
  - *Network layer*, die von Ereignissen verwendet wird, die sich mit dem ausgewählten Zeitraum überlappen.
  - *Transport layer*, die von Ereignissen verwendet wird, die sich mit dem ausgewählten Zeitraum überlappen.
  - *Application layer*, die von Ereignissen verwendet wird, die sich mit dem ausgewählten Zeitraum überlappen.
  - *Service*, die von Ereignissen verwendet werden, die sich mit dem ausgewählten Zeitraum überlappen.
- Dashboards filtern nun Schwachstellen heraus, die mit Status *Resolved* markiert sind.
- Die zugehörige Terminologie wurde von *Schwachstellen* (*von Schwachstellen betroffene Assets*) zu *Exposures* (*exponierte/gefährdete Assets*) umbenannt.
- Die Leistung des Dashboard-Panels wurde für Umgebungen mit vielen betroffenen Assets verbessert. In diesem Zusammenhang wurde die Speichernutzung für das Schwachstellen-Matching optimiert.
- Die Lesbarkeit von exportierten PDF-Reports wurde durch eine optimierte Tabellengenerierung verbessert.
- Die Konfiguration der E-Mail-Integration von Grafana Alerting wurde vereinfacht.

8. Neue Vulnerability-Seite

Informationen zu Schwachstellen wurden aus dem Grafana-Dashboard in einen eigenen Bereich verschoben, sodass Sie leichter auf Details zugreifen, Risiken verwalten und direkt dort Maßnahmen ergreifen können, wo es nötig ist:



- **Neuer Tab *Vulnerability details***: Detailinformationen zu den Schwachstellen werden nun in einem eigenen Tab auf der Seite *Vulnerability* präsentiert. Sie wurden aus dem Dashboard *Vulnerability* in Grafana entfernt.
- **Neuer Tab *Affected assets***: Die betroffenen Assets einer Schwachstelle sind nun auf der Seite *Vulnerability* zu finden und wurden aus dem Dashboard *Vulnerability* in Grafana entfernt. Unter dem Tab finden Sie detaillierte Informationen zu den von Schwachstellen betroffenen Assets, einschließlich Daten der Sensor- und Netzwerk-Schnittstellen. Außerdem wird das Expositions-

Management integriert, mit dem sämtliche Schwachstellen bewertet und behandelt sowie Lösungen mit transparenten Begründungen zugewiesen werden können. (siehe Lösung von Schwachstellen mithilfe von Statusangaben oben).

> **Neuer Tab *Security advisory document***: Auch die Sicherheitshinweise der Hersteller (Security advisories) sind nun auf der Seite *Vulnerability* zu finden und wurden aus dem Dashboard *Vulnerability* in Grafana entfernt.

9. Beschleunigte Leistungsfähigkeit des Schwachstellen-Matchings

Die Geschwindigkeit des Matchings von Schwachstellen zu den vorhandenen Assets wurde weiter erhöht – teilweise sehr deutlich. Dies beschleunigt die Abläufe für die Analyse und Behandlung der für die Anlage relevanten Schwachstellen.

10. Update von Komponenten

> Keycloak wurde von 23.0.7 auf 26.0.5 aktualisiert.
> Grafana wurde von 11.0.0 auf 11.2.4 aktualisiert.

11. Fehlerbehebungen und kleine Verbesserungen

Es wurden viele kleinere Korrekturen und Verbesserungen vorgenommen.

12. Produktlebenszyklus- und Supporthinweis

Das Update von StationGuard GridOps 1.20 auf Version 2.00 ist kostenlos. Die StationGuard-GridOps-Version 2.00 löst Version 1.20 als Service-Basisversion ab. Wir empfehlen Ihnen, alle Ihre Installationen auf die Version 2.00 zu aktualisieren.

Wir bei OMICRON nehmen jede Art von Schwachstelle, die unsere Produkte betrifft, sehr ernst und freuen uns über jede Meldung, die uns hilft, deren Sicherheit zu verbessern. Aus diesem Grund haben wir einen systematischen Ansatz für den Erhalt, die Verarbeitung und die Bekanntgabe solcher Schwachstellen-informationen entwickelt.
Bitte besuchen Sie https://www.omicronenergy.com/de/support/product-security für weitere Informationen.

Bisherige Versionen

	Schwerpunkt	Veröffentlicht im
Version 1.20	Optimierte Schwachstellen-Datenbank	März 2024
Version 1.10	Verbesserungen der Nutzbarkeit	Dezember 2023
Version 1.00	Software Release	Dezember 2022

Version 1.20

1. Neue Security Advisories im Schwachstellenkatalog

Der Schwachstellenkatalog wurde um folgende Hersteller erweitert, wobei die jüngsten Neuzugänge **fett** hervorgehoben sind:

Vendors		
ABB	**HMS Networks**	**PSI GridConnect**
Advantech	**Honeywell**	**Rockwell**
A. Eberle	**IPCOMM**	**SAE IT-systems**
Beckhoff	**Landis+Gyr**	Schneider Electric
Cisco	**Meinberg**	**Schweitzer Engineering Laboratories**
Delta Electronics	Moxa	Siemens
EFACEC	**mySCADA**	Sprecher Automation
Fortinet	**Nari**	Vivavis
General Electric (Gas Power)	**Nokia**	**WAGO**
General Electric (Grid Solution)	OMICRON	Westermo
Hirschmann/Belden/ProSoft	**Panasonic**	**Wibu-Systems**
Hitachi Energy	**Phoenix Contact**	

> Gesamtzahl der Security Advisories: **4.210+**
> Gesamtzahl erkennbarer Schwachstellen: **9.940+**

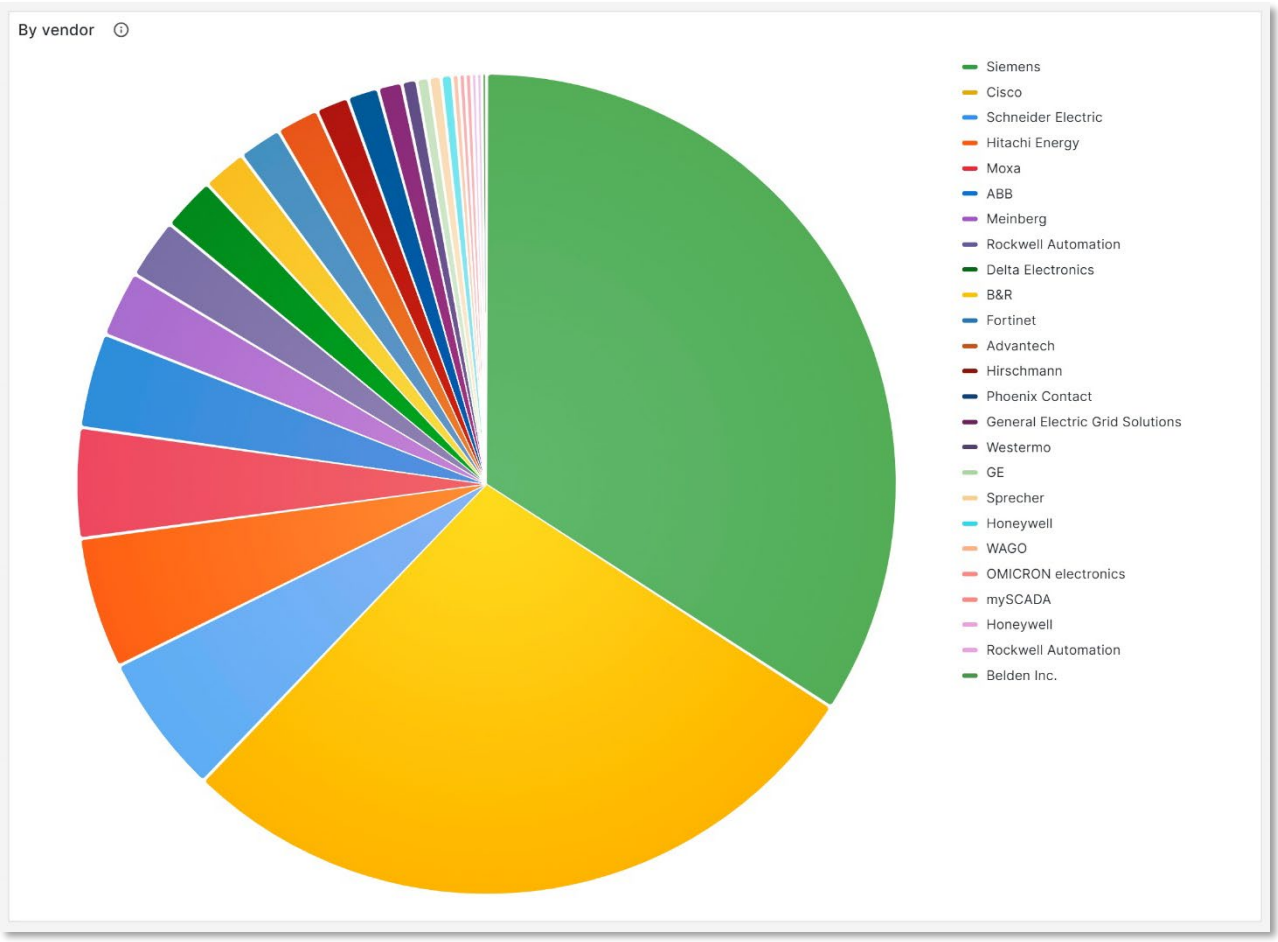


Abbildung 1: Schwachstellen nach Hersteller

2. Beschleunigtes Matching von Schwachstellen

Wir haben die Geschwindigkeit des Matchings bei verschiedenen Anbietern optimiert:

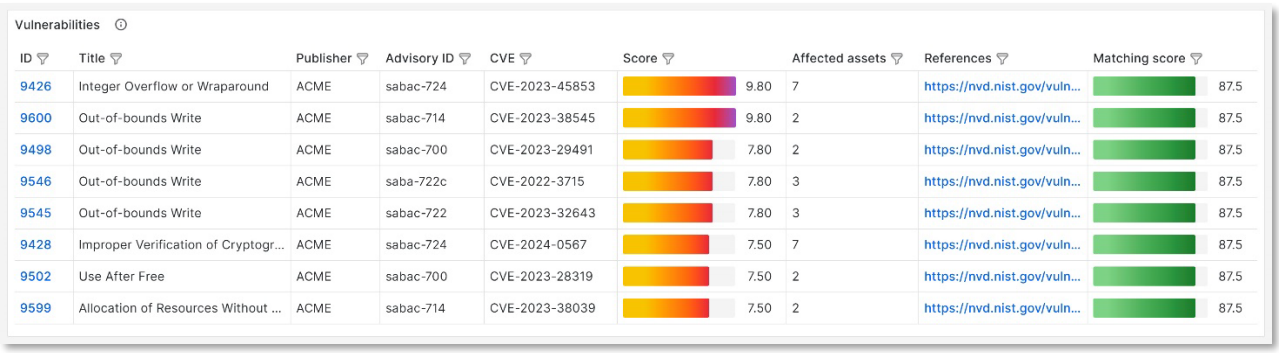
- **Cisco** ~20x schneller
- **Siemens** ~10x schneller
- **ABB** ~5x schneller
- **Hitachi** ~5x schneller
- **Schneider** ~5x schneller
- **Moxa** ~3x schneller
- **Hirschmann** ~2x schneller

Die Dauer des Matchings konnte erheblich reduziert werden, von 1 bis 900 Sekunden auf 1 bis 50 Sekunden pro Asset, je nach Asset-Bestand. Bei 100 Assets dauert der Prozess jetzt im Durchschnitt etwa 15 Minuten. Es ist wichtig zu beachten, dass die Geschwindigkeit des Prozesses direkt von der Vollständigkeit, Genauigkeit und Sorgfalt des Asset-Inventars abhängt.

3. Höchste Genauigkeit für umfassendes Schwachstellen-Matching

Wir haben Funktionen implementiert, um die Genauigkeit unserer Daten zu verbessern. Insbesondere haben wir die Präzision des Matchings von Sicherheitsrisiken verbessert. Um eine umfassende Abdeckung unserer Daten zu gewährleisten, unterscheiden wir zwischen verschiedenen Gerätefamilien und Versionen. Hier sind ein paar Beispiele:

Vendor	Enhancements
General Electric (Grid Solution)	> Multilin-, UR-, URplus- und SR-Gerätefamilien hinzugefügt.
Meinberg	> Gerätefamilien LANTIME, IMS und SyncFire sowie das Betriebssystem LTOS hinzugefügt.
Siemens	> Unterscheidung zwischen A8000 CP-800x/802x und CP-803x/805x. > RUGGEDCOM RS900 entspricht nun den Empfehlungen für RS9xx.
Westermo	> Unterscheidung zwischen WeOS-Version 4.X und 5.X. > Wolverine-Gerätefamilien hinzugefügt.



Vulnerabilities

ID	Title	Publisher	Advisory ID	CVE	Score	Affected assets	References	Matching score
9426	Integer Overflow or Wraparound	ACME	sabac-724	CVE-2023-45853	9.80	7	https://nvd.nist.gov/vuln...	87.5
9600	Out-of-bounds Write	ACME	sabac-714	CVE-2023-38545	9.80	2	https://nvd.nist.gov/vuln...	87.5
9498	Out-of-bounds Write	ACME	sabac-700	CVE-2023-29491	7.80	2	https://nvd.nist.gov/vuln...	87.5
9546	Out-of-bounds Write	ACME	saba-722c	CVE-2022-3715	7.80	3	https://nvd.nist.gov/vuln...	87.5
9545	Out-of-bounds Write	ACME	sabac-722	CVE-2023-32643	7.80	3	https://nvd.nist.gov/vuln...	87.5
9428	Improper Verification of Cryptogr...	ACME	sabac-724	CVE-2024-0567	7.50	7	https://nvd.nist.gov/vuln...	87.5
9502	Use After Free	ACME	sabac-700	CVE-2023-28319	7.50	2	https://nvd.nist.gov/vuln...	87.5
9599	Allocation of Resources Without ...	ACME	sabac-714	CVE-2023-38039	7.50	2	https://nvd.nist.gov/vuln...	87.5

Abbildung 2: Beispiel für Schwachstellen mit Schweregrad und zugehöriger Bewertung

4. Beispielhafte Vorgehensweise für den Umgang mit Inventardaten

Die Dokumentation enthält Vorschläge zur Verbesserung der Asset-Daten, um die Genauigkeit des Schwachstellen-Matchings zu erhöhen. Weitere Informationen finden Sie unter „*Help* > *GridOps assets* > *Vulnerability matching* > *Best practices*".

5. Verkürzte Ladezeit des *Event*-Dashboards

Die Ladezeit des *Event*-Dashboards wurde durch die Optimierung der Abfragen für größere Datensätze reduziert.

6. Anzeige der Suchergebnisse für unvollständige Schwachstellen und Advisories

Bisher konnte es vorkommen, dass einige Schwachstellen und Advisories bei der Abfrage im Suchfeld des *Vulnerability Catalog Dashboard* nicht richtig dargestellt wurden. Jetzt werden alle passenden Schwachstellen und Avisories in den Ergebnissen angezeigt.

7. Standardintervalle für das automatische Update von Dashboards

Die Intervalle für das automatische Update sind nun für alle Dashboards auf eine Minute festgelegt, um ein vorhersehbares Verhalten sicherzustellen. Es ist weiterhin möglich, die Intervalle für jedes Dashboard individuell anzupassen.

8. Erweiterter Speicherplatz

Wenn Sie die virtuelle Festplattengröße erweitern, nutzt GridOps automatisch den zusätzlichen Speicherplatz. Weitere Details finden Sie unter „*Help* > *GridOps platform* > *Expanding the storage space*".

9. Fehlerbehebungen und kleine Verbesserungen

- Betriebssystem erholt sich ordnungsgemäß, wenn während des Starts ein vorzeitiger Neustart ausgelöst wird.
- Die Zuverlässigkeit der initialen Sensorverbindung wurde verbessert.
- Und viele andere kleinere Korrekturen und Verbesserungen.

10. Update von Komponenten

- Keycloak wurde von 21.1.1 auf 23.0.7 aktualisiert.

Version 1.10

1. Neue Security Advisories im Schwachstellenkatalog

Der Schwachstellenkatalog wurde um folgende Hersteller erweitert:

Vendors		
ABB	Hirschmann/Belden/ProSoft	Siemens
A. Eberle	Hitachi Energy	Sprecher Automation
Cisco	Moxa	Vivavis
Fortinet	OMICRON	Westermo
General Electric (Gas Power)	Schneider Electric	

> Gesamtzahl der Security Advisories: **3.527**
> Gesamtzahl erkennbarer Schwachstellen: **7.796**

2. Verbessertes Schwachstellen-Matching

Wir haben Funktionen zur Verbesserung der Datengenauigkeit implementiert, die insbesondere auf die Genauigkeit des Matchings von Schwachstellen und die Geschwindigkeit abzielen. Hier sind ein paar Beispiele:

Vendor	Enhancements
Hitachi / ABB	> Relion-Gerätefamilien hinzugefügt.
Schneider	> P30- und P40-Gerätefamilien hinzugefügt.
Siemens	> RUGGEDCOM-Gerätefamilien hinzugefügt. > SIPROTEC 4/5/Compact-Gerätefamilien hinzugefügt. > Matching der Module CP050, CP100, CP200, CP300 und EN100 zu den entsprechenden Geräten.
Westermo	> Lynx-, RedFox-, und RFIR -Gerätefamilien hinzugefügt.

3. Verkürzte Ladezeit für Dashboards

Die Leistung der Dashboard-Abfrage wurde verbessert und das Matching von Datenpunkten optimiert, was zu einer schnelleren Ladezeit für alle Dashboards führt.

4. Verweis auf Security Advisories im *Vulnerability Dashboard*

Das *Vulnerability Dashboard* enthält jetzt einen Verweis auf das entsprechende Security Advisory.

5. Gezieltere Filterung in Dashboards

Die Dashboard-Filter wurden vereinfacht und erweitert. Dadurch ist es nun komfortabler, die Ergebnisse einzugrenzen und zu kontrollieren.

6. Update von GridOps

Ab Version 1.10 ist es möglich, GridOps über das Webinterface zu aktualisieren. Weitere Details finden Sie unter „*Help* > *GridOps platform* > *Updating GridOps*". Außerdem wurde die Größe des Installations-Images von ~8 GB auf ~3 GB reduziert, um den Bereitstellungsprozess zu beschleunigen.

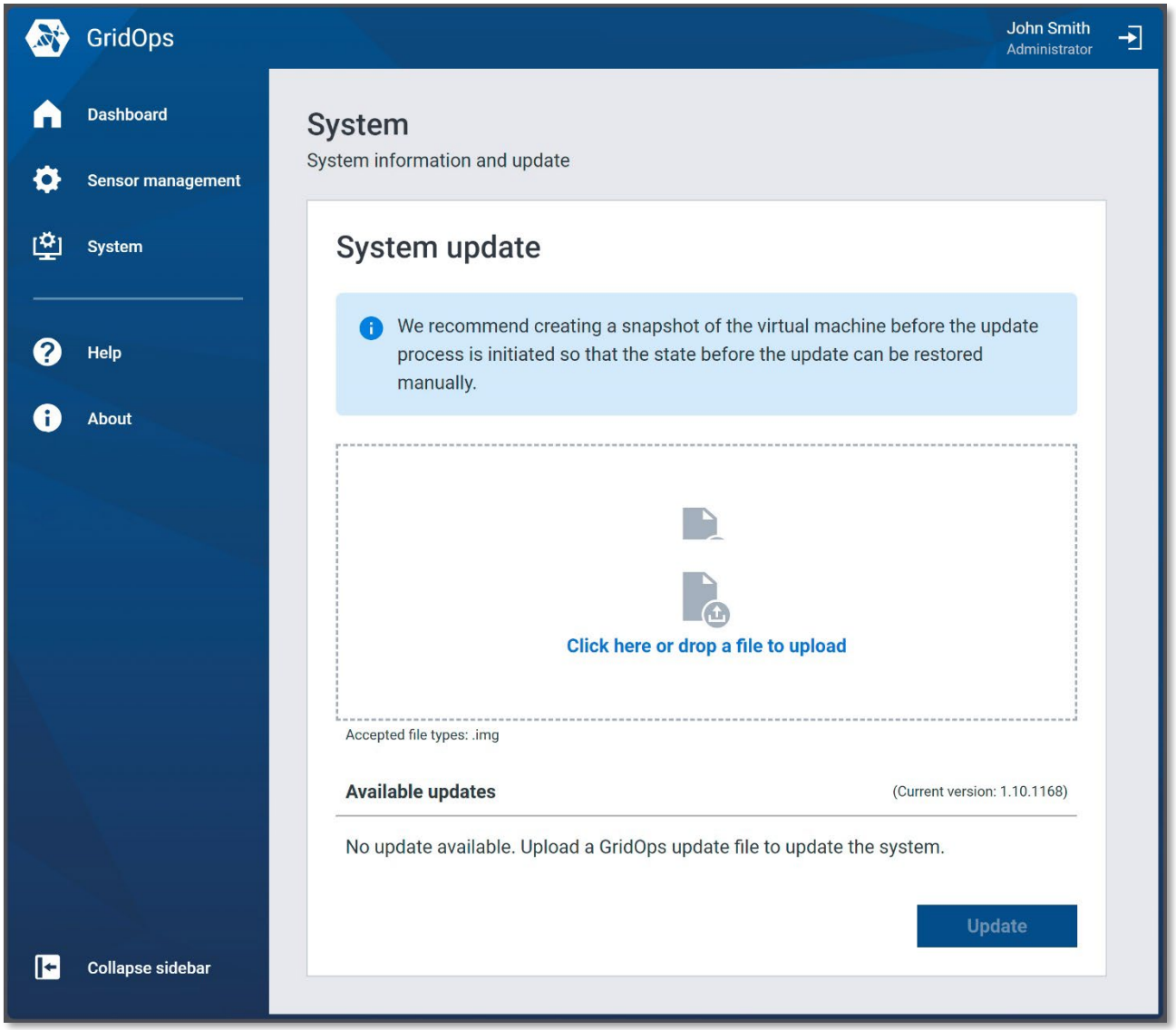


Abbildung 3: GridOps-Update

7. Volle Unterstützung für StationGuard 2.30 Nachrichten

StationGuard 2.30-Nachrichten werden mit integrierten Zeitstempeln für die Nachrichten und einer Protokollierung der Sensorkonfiguration vollständig unterstützt. StationGuard 2.20-Meldungen werden allerdings nur teilweise unterstützt, da die Sensorkonfigurationen nicht mehr aktualisiert werden.

8. Vereinfachte Nachverfolgung von unbestätigten und aktiven Ereignissen

Die Ereignisse enthalten nun einen Zeitstempel, um die Verfolgung von unbestätigten und aktiven Ereignissen zu verbessern. Dies ermöglicht eine genauere Analyse der Ereignisse.

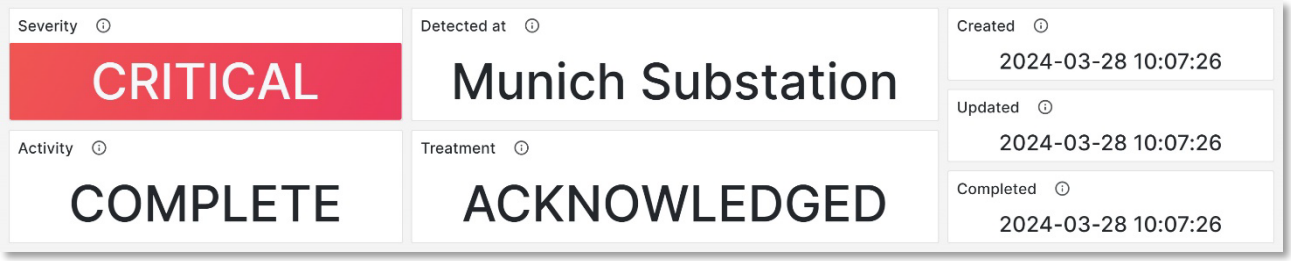


Abbildung 4: Ereignisse mit Zeitstempel

9. Erweiterter Zugang zum Identitäts- und Zugriffsmanagement

GridOps-Administratoren haben nun erweiterten Zugriff auf die Keycloak-Einstellungen. Dadurch ist eine tiefere Kontrolle und Anpassung des Identitäts- und Zugriffsmanagements möglich, zum Beispiel die Verwaltung von OpenID Connect-Clients. Weitere Details finden Sie unter „*Help* > *GridOps platform* > *Keycloak identity and access management”*.

10. Datenspeicherung

Um genügend Speicherplatz sicherzustellen, optimiert GridOps automatisch die Datenaufbewahrung. Dabei werden die ältesten Daten gelöscht, bis wieder ausreichend Speicherplatz vorhanden ist. Weitere Details finden Sie unter „*Help* > *GridOps platform* > *Data retention*”.

11. Fehlerbehebungen und kleine Verbesserungen

- Die GridOps-Dienste haben sich nun vollständig von unerwarteten Aktionen der Benutzenden erholt, wie zum Beispiel Systemstartunterbrechungen.
- TLSv1 TLSv1.1 TLSv1.2 wurden deaktiviert. Es wird nur noch TLSv1.3 verwendet, das eine perfekte Vorwärtsverschlüsselung gewährleistet.
- Und viele andere kleinere Korrekturen und Verbesserungen.

12. Update von Komponenten

- Keycloak wurde von 20.0.2 auf 21.1.1. aktualisiert.
- Grafana wurde von 9.3.6 auf 10.2.2. aktualisiert.

Version 1.00

Dies ist die erste Version der GridOps-Software, dem zentralen Managementsystem für StationGuard. GridOps wurde als Reaktion auf Anfragen von StationGuard-Kund:innen entwickelt.

1. Das zentrale Managementsystem für StationGuard

GridOps kann als zentrales Managementsystem für StationGuard die OT-Netzwerke auf mehreren Dashboards mit unterschiedlichen Ansichten visualisieren. Ein Dashboard kann beispielsweise den globalen Asset-Bestand anzeigen, während ein anderes alle Alarme für ein bestimmtes Netzwerk anzeigt.

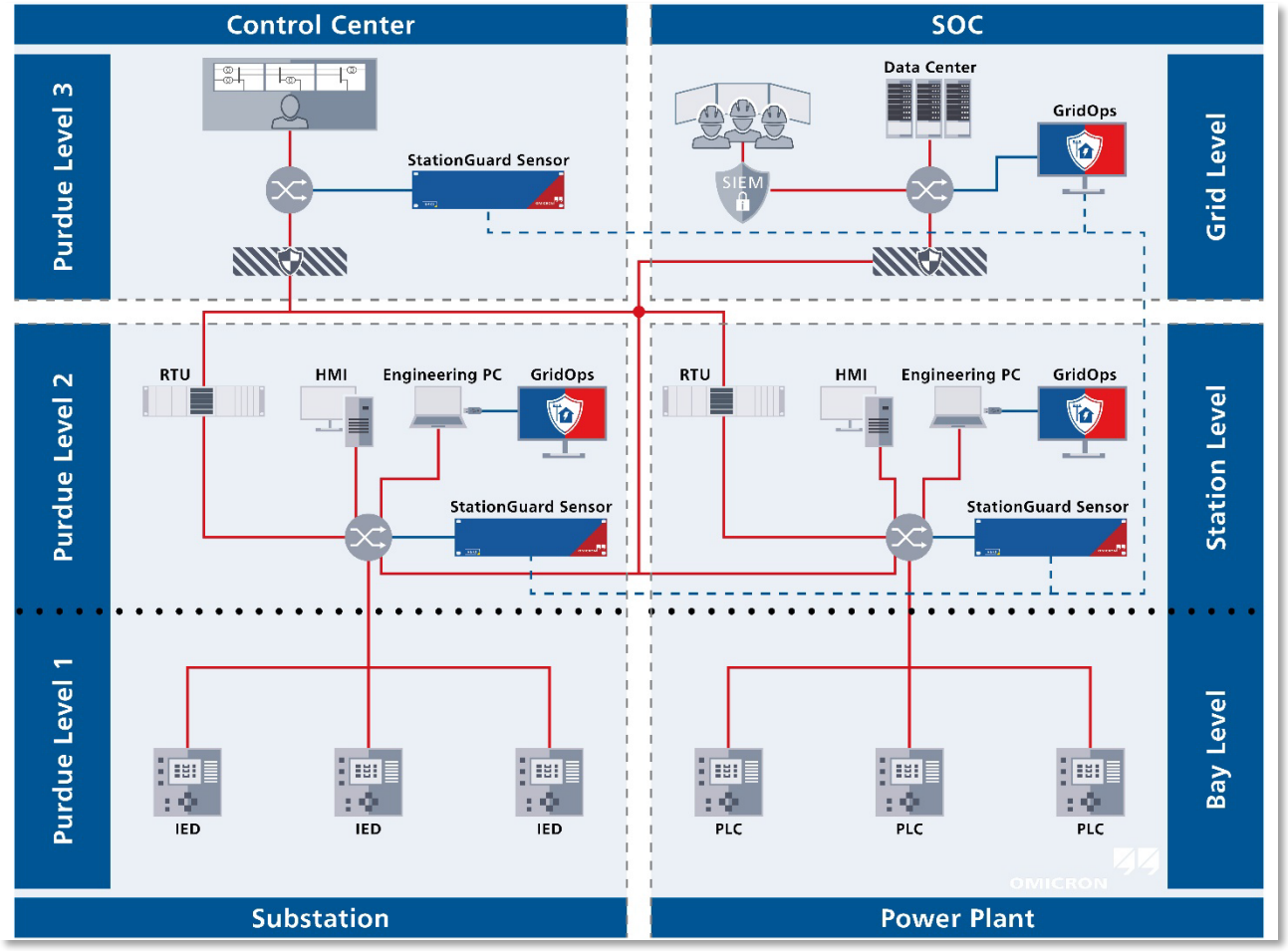


Abbildung 5: Typischer Aufbau von GridOps mit StationGuard

2. Netzweite Sichtbarkeit

GridOps-Dashboards bieten einen einfachen Zugriff auf den Alarmstatus im gesamten Netz. Sie können schnell erkennen, ob es an einem bestimmten Ort oder zu einer bestimmten Zeit wichtige Alarme gibt. Die Plattform bietet eine Vielzahl von Visualisierungs- und Analyseoptionen für die Analyse von aktuellen und historischen Ereignissen. GridOps führt außerdem eine Datenbank mit allen Ereignissen und Aktivitäten, die über alle Sensoren hinweg aufgetreten sind.

Dies ermöglicht es Ihnen, Ereignisse, die zuvor an allen Standorten, an denen Sensoren installiert sind, aufgezeichnet wurden, anzuzeigen und zu durchsuchen. Das *Alert Overview Dashboard* veranschaulicht mithilfe von Zeitreihen- und Kuchendiagrammen, wie verschiedene Arten von Alarmen je nach Art und geografischem Bereich im OT-Netzwerk verteilt sind.

Sie können auch sehen, wie sich diese Alarme auf verschiedene Asset-Typen beziehen. Außerdem wird deutlich, wie sie miteinander in Beziehung stehen. Die Häufigkeit von Alarmen kann als Teil des Vorfallsanalyseprozesses untersucht werden.

Durch die Analyse von Ereignisdaten können Sie Trends erkennen, die auf der Grundlage der bisher gesammelten Daten analysiert werden können. Es ist möglich, Muster und anomale Aktivitäten zu ermitteln, die bei der Identifizierung verdächtiger Aktivitäten helfen können. Sie können außerdem alle Betriebsereignisse (*Functional Events*) analysieren, die von StationGuard aufgezeichnet wurden. Dazu gehören erfolgreiche und fehlgeschlagene Schaltvorgänge sowie heruntergeladene Fehleraufzeichnungen.

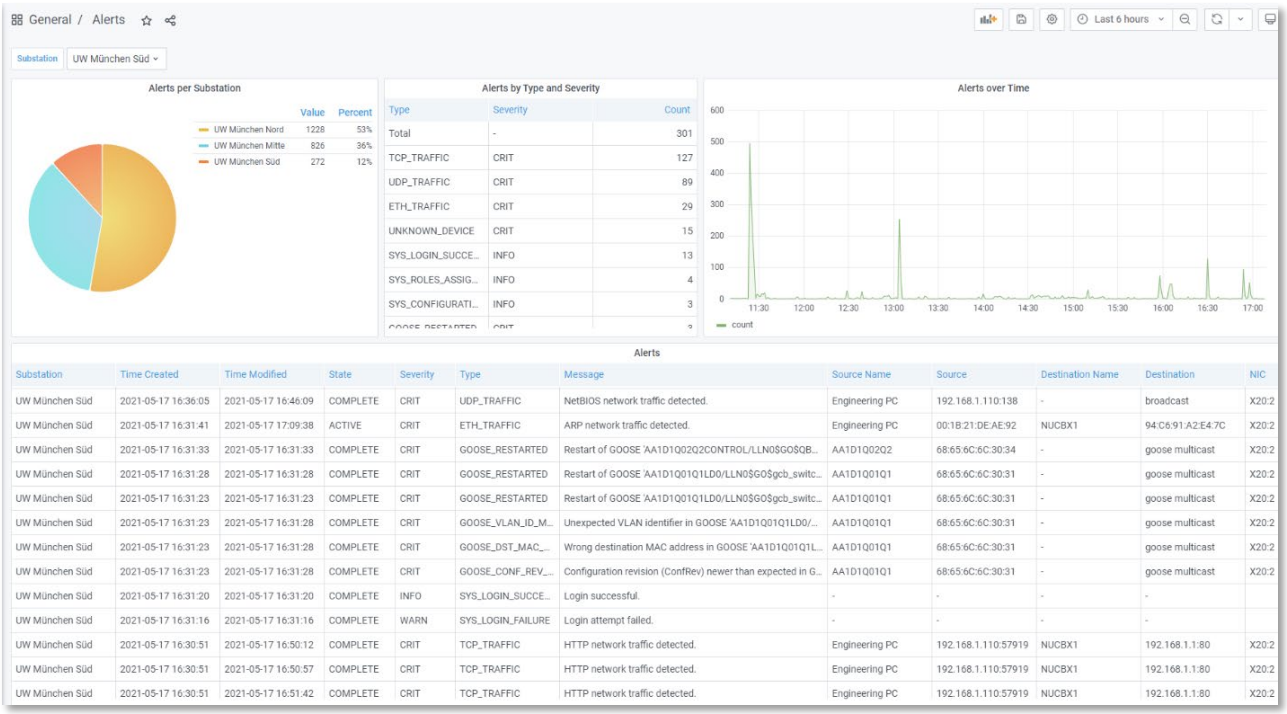


Abbildung 6: Übersicht der Warnmeldungen

3. Globales Asset-Inventar

Die GridOps-Plattform erstellt ein globales Asset-Inventar durch die Kombination der Daten aller StationGuard-Sensoren, die über das gesamte Netzwerk verteilt sind. Sie können diese Daten suchen und anzeigen lassen. Das Asset-Inventar wird in Echtzeit mit Informationen von allen an das System angeschlossenen IDS-Sensoren aktualisiert. Eine Tabelle gibt einen Überblick über alle Asset-Eigenschaften, wobei Filteroptionen zur Verfügung stehen, um bestimmte Asset-Typen zu finden.

Durch die Kombination all dieser Funktionen und der unübertroffenen Fähigkeit von StationGuard, Daten aus SCL-Dateien oder Asset-Dokumenten zu importieren, die Informationen über das Asset-Inventar enthalten, können Sie sich – unerheblich, ob Sie OT oder Cybersicherheits:expert:in sind – jederzeit ein detailliertes Bild von ihren Assets machen und alle Sicherheits- oder Funktionsprobleme angehen.

Für ein effektives Risiko- und Schwachstellenmanagement sind umfassende Daten über jedes Asset unerlässlich. Sie können Schwachstellen besser priorisieren und analysieren, je mehr Informationen Sie über ein bestimmtes Asset haben. Dadurch wird die Schwachstellenbewertung aufschlussreicher.

Mit der mobilen Version von StationGuard für die MBX1-Plattform können Netzwerke gescannt werden, in denen kein fester (IDS-)Sensor installiert ist. Die gescannten Netzwerke werden automatisch zum Inventar hinzugefügt.

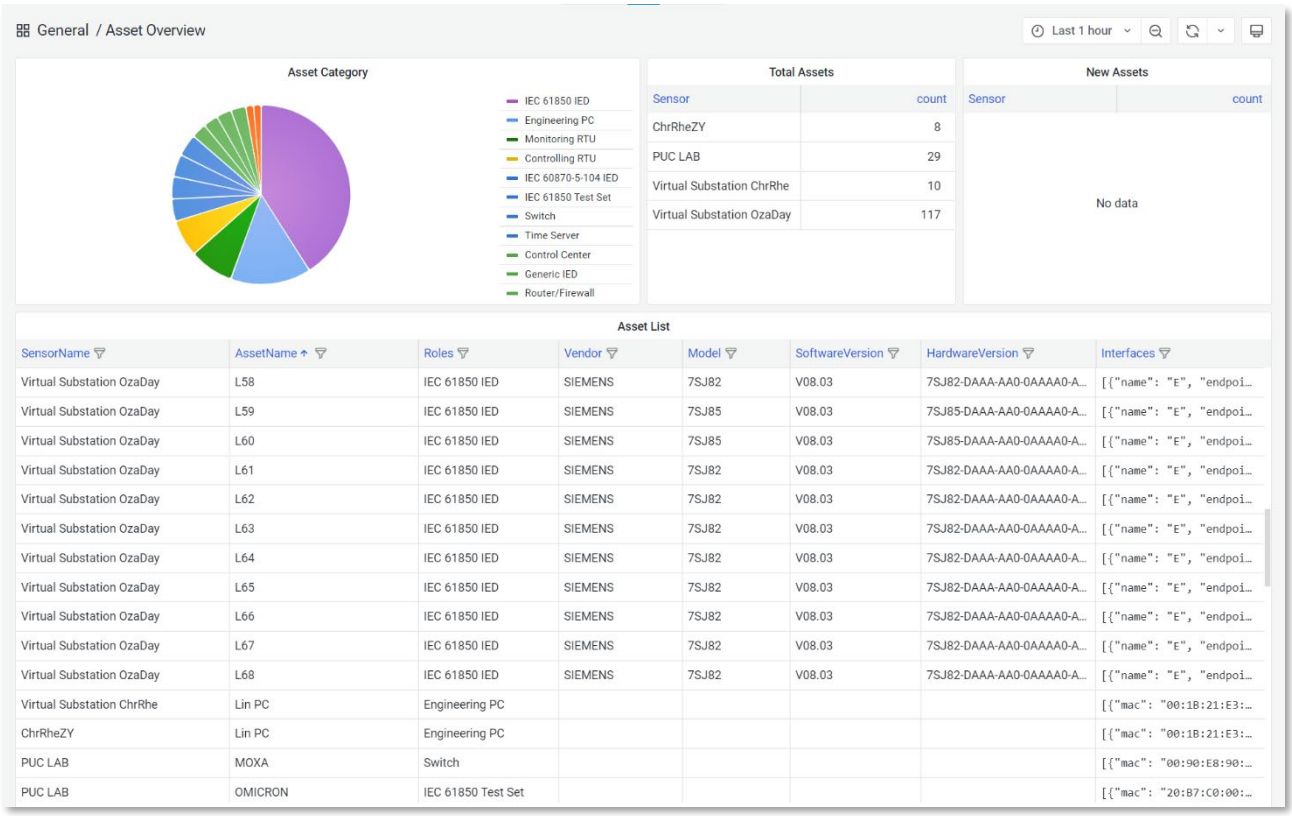


Abbildung 7: Überblick der Assets

4. Schachstellen-Management

Ein wichtiger Schwerpunkt des Schwachstellenmanagements ist die Identifizierung, Bewertung, Meldung, Verwaltung und Behebung von Schwachstellen, die in einer Reihe von Geräten und Assets innerhalb eines Netzwerks als Teil eines kontinuierlichen Prozesses auftreten. Die Aufgabe, gemeldete Schwachstellen von Schutz- und Automatisierungsgeräten mit den tatsächlich im Feld installierten Geräten abzugleichen, stellt eine unerwartet große Herausforderung dar.

Bei der Bewertung einer Schwachstelle sind mehrere Faktoren zu berücksichtigen. Der erste Schritt ist die Identifizierung des Gerätetyps und der darauf installierten Firmware-Version. Außerdem ist es wichtig zu wissen, ob bestimmte Netzwerk- und CPU-Module auf dem Gerät installiert und aktiviert sind.

Erschwerend kommt hinzu, dass Security Advisories nicht immer so genau sind, wie sie sein sollten. GridOps Schwachstellenmanagement liefert aber auch hier eine Lösung. Es berücksichtigt die Auswirkungen mehrerer Common Vulnerability Exposures (CVEs) und bestimmt, welche IEDs von einem bestimmten CVE oder Security-Advisory betroffen sind. Dadurch können Sie genauer bestimmen, ob ein IED verwundbar ist und wenn ja, in welchem Ausmaß. Das *Vulnerabilities Dashboard* bietet einen Überblick über die Gesamtschwachstellenbelastung, die Patchbarkeit und den Gefährdungsgrad der Schwachstellen.

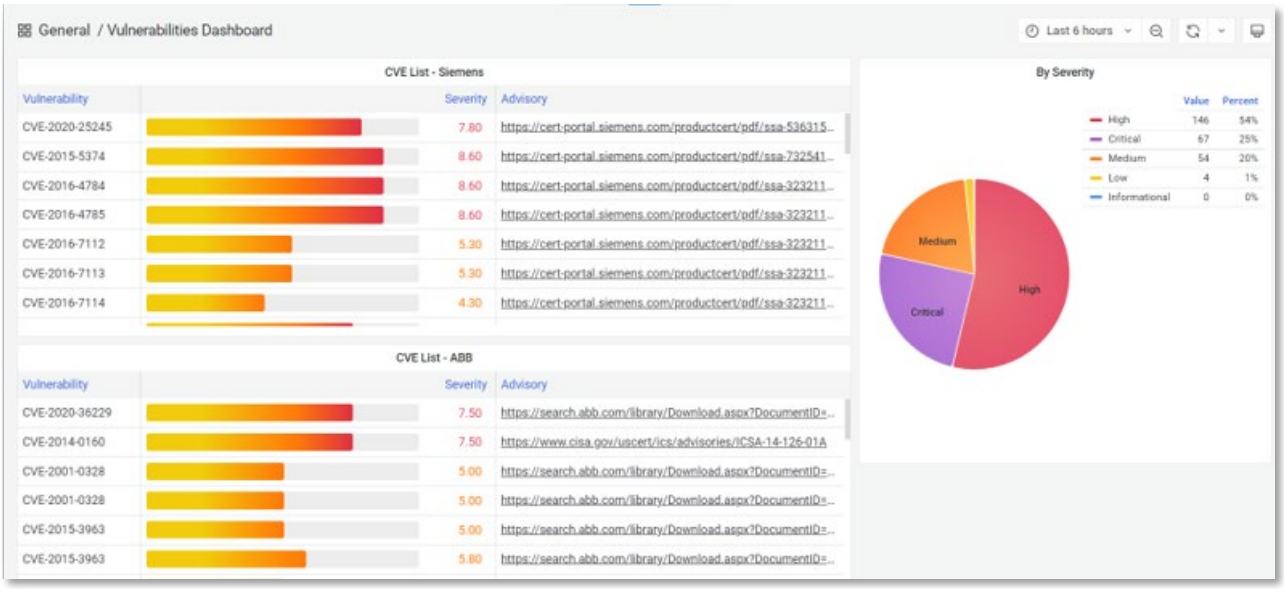


Abbildung 8: Vulnerabilities Dashboard

5. Berichtserstellung

GridOps erstellt Berichte. Diese Berichte geben Ihnen frühzeitig Einblicke in Cybersicherheitstrends, funktionale Probleme, Statistiken, Ihren Asset-Bestand und die damit verbundenen Schwachstellen. Sie ermöglichen es Ihnen, den Zustand Ihrer Risikolage zum Zeitpunkt der Analyse dieser Berichte zu dokumentieren. Zudem werden umfassende und aussagekräftige Risikobewertungen erstellt. Diese können der Geschäftsleitung, den Anbietern und den Aufsichtsbehörden vorgelegt werden. Dadurch wird eine Priorisierung und Minderung der Risiken ermöglicht.

6. Tiefgreifende Analyse von der Station bis zum Stromnetz

Die Visualisierung von Stromnetz-OT-Netzwerken durch StationGuard ist einzigartig und interessant für Stromnetz-OT-Expert:innen sowie IT-Verantwortliche. Das Netzwerk wird grafisch dargestellt und enthält eine vollständige Liste aller Geräte im Netzwerk mit ihrer Position. Mit GridOps können Sie Alarme und Ereignisse in den OT-Netzwerken global analysieren und die Standorte der IDS-Sensoren in jedem OT-Netzwerk auf Sensorebene visualisieren.

Es gibt eine Visualisierungsoption, die dem Liniendiagramm und der technischen Dokumentation des Systems ähnelt: das ZeroLine-Diagramm. ZeroLine-Diagramme können automatisch aus den Engineering-Dateien der Anlage generiert werden oder manuell strukturiert werden. Es ist empfehlenswert, dass sie entweder der Netzwerkstruktur nach dem Purdue-Modell oder dem elektrischen Layout der Anlage nahekommen.

GridOps bietet einen umfassenden Analyse- und Untersuchungsansatz, um aufkommende Bedrohungen zeitnah anzugehen. Es ist jetzt möglich, alle Alarme einzusehen. Dazu navigieren Sie von einer Übersicht auf Netzebene zu einer bestimmten Leitstellen-, Kraftwerks- oder Umspannwerksnetzansicht und verwenden dabei die bekannte StationGuard ZeroLine-Diagrammvisualisierung.

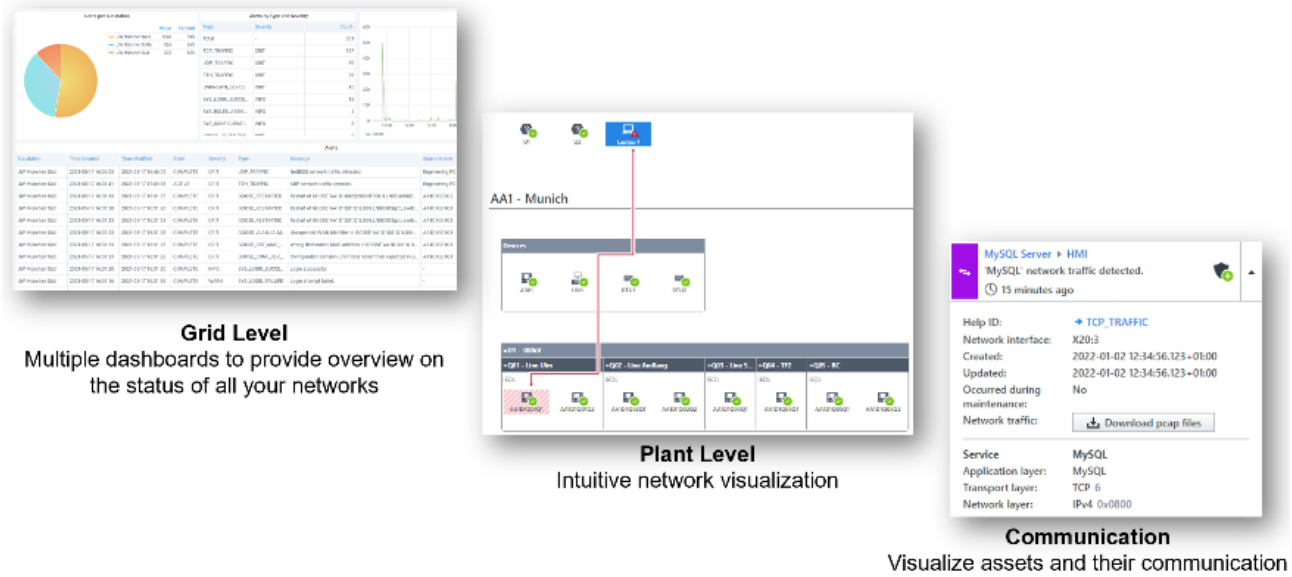


Abbildung 9: Darstellungen für Netzebene Anlagenebene und Kommunikation

7. Active Directory-Integration und rollenbasierte Zugriffskontrolle

LDAP ist ein Protokoll, das genutzt werden kann, um GridOps in eine Active Directory-Umgebung zu integrieren. StationGuard weist verschiedenen Benutzer:innen bestimmte Rollen zu, um den Zugriff auf verschiedene Funktionen zu regeln, die für die Anzeige und Konfiguration von StationGuard-Instanzen zur Verfügung stehen. Die Benutzer:innen haben unterschiedliche Zugriffsebenen auf verschiedene Funktionen.

So beschränken wir, welche Funktionen für welche Benutzer:innen verfügbar sind und begrenzen ihre Nutzung. Außerdem können Sie über die lokale StationGuard-Client-Bedienoberfläche auf StationGuard IDS-Sensoren zugreifen, falls die Verbindung zur zentralen GridOps-Instanz aus irgendeinem Grund nicht verfügbar ist. So haben Sie stets die Möglichkeit, separat auf die Sensoren zuzugreifen, wenn Sie dies wünschen.

Für weitere Informationen, zusätzliche Literatur
und detaillierte Kontaktdaten unserer weltweiten
Standorte besuchen Sie bitte unsere Websites:

www.omicroncybersecurity.com
www.omicronenergy.com